Bennett-Carper Data Security Act of 2006
Frequently Asked Questions

Who is covered by the Data Security Act of 2006?

Financial institutions, their affiliates and any other entities engaged in any financial activities described in Section 4(k) of the Bank Holding Company Act.

Any other entity, including federal agencies, that maintains or communicates covered information.

What types of information are covered?

Any information that could be used to commit identity theft or account fraud would be covered.

Sensitive personal information – first and last name, address or telephone number, in combination with 1. Social Security Number (SSN), 2. Drivers License Number (DLN), or 3.Taxpayer Identification Number (TIN). There is an exception for publicly available information.

Sensitive account information – financial account numbers relating to a consumer, including a credit or debit card number, in combination with any security code, access code, password or other personal identification information required to access the financial account.

What are the safeguarding or security requirements of covered entities?

All covered entities would be required to put in safeguards to protect all sensitive personal or account information.

The functional regulators would craft the detailed safeguarding requirements for their covered entities based upon the size and the complexity of the entity and the sensitivity of the consumer information.

Are electronic and paper records covered?

Both electronic and paper records are covered.

What is the trigger for consumer notification of a breach?

The trigger would be based on the likelihood that the breach of information will lead to "substantial harm or inconvenience" due to identity theft or account fraud.

"**Substantial harm or inconvenience**" includes identity theft or account fraud situations where consumers experience financial loss

or are forced to expend significant time and effort to correct false information.

Broad consumer notice would not be required if the information stolen was not useable to the thief, through encryption for example, or if it is not enough to steal someone's identity or engage in fraudulent credit card, debit card or other transactions. For instance, notice would not be required in a situation where the consumer merely receives a replacement credit or debit card since there was no financial loss and little if any inconvenience.

How will notification work?

Functional regulators would prescribe regulations regarding method, content and timing of notifications required to consumers.

What is a functional regulator?

The state or federal entity charged to oversee operations and business practices of covered entities.

For example, FDIC, Federal Reserve, and OCC would oversee most financial institutions. Other entities will fall within the enforcement jurisdiction of Federal Trade Commission (FTC). Federal agencies are internally regulated.

Is there a preemption of existing state laws?

All state laws relating to security and breach notification are preempted to create a uniform national standard.

Although some of these laws contain similar elements, many have inconsistent and conflicting standards. Different state laws result in higher costs and uneven consumer protection. The need to track multiple state laws is particularly difficult for smaller institutions and could lead to consumer delays in receiving timely notices.

Who will enforce this law?

The bill is based upon the GLB model and will be enforced exclusively by the functional regulator of the covered entity.

Why is there a safe harbor for some financial institutions?

Many financial institutions already have a safeguarding requirement and breach notification regime in place under GLB law, regulations and guidance. It is a system that is working and is in fact the model for this legislation. There is no need to rewrite those laws or regulations as they relate to safeguarding or breach notification.